Cyber spazio: un nuovo incubatore di rischi

Il Cyber spazio, inteso come il "luogo" che comprende tutti "i sistemi digitali di connessione, acquisizione e condivisione delle informazioni", sta diventando uno dei più efficaci incubatori di nuove minacce alle imprese e agli Stati. All'interno del network delle relazioni tra sistemi si stanno verificando episodi sempre più frequenti ed efficaci di attacchi devastanti ai sistemi economici e a quelli strategici di interesse nazionale. Anzi, dopo la fase pioneristica in cui si è assistito alla trasposizione nel nuovo territorio delle tradizionali azioni criminali, si stanno consolidando nuove modalità di comportamento capaci di adattarsi e trarre vantaggio dal contesto tecnologico a cui i sistemi economici, politici e militari fanno sempre più affidamento. Secondo alcune ricerche questo fenomeno conoscerà una crescita esponenziale: nel 2019, il cyber crime costerà alle imprese 2.100 miliardi di dollari, una somma pari quasi al PIL dell'Italia, con una quadruplicazione dei valori rispetto al 2015.
L'ambito economico è purtroppo però solo uno dei piani in cui si giocherà la nuova partita che forse genererà a livello del confronto tra gli Stati il rischio con maggior potenziale sistemico.
Per queste ragioni non possiamo relegare agli esperti della materia l'interpretazione delle tendenze in atto: non è forse lontano il momento in cui l'analisi fondamentale delle imprese dovrà considerare la loro capacità di reazione degli attacchi informatici al pari della loro struttura del debito, della capacità competitiva, ecc.

Cyber crime, cyber attack cyber security tanti neologismi per definire una nuova classe di rischi

I sistemi economici, finanziari e sociali vanno evolvendosi secondo una crescita esponenziale del numero, della qualità e della intensità delle loro interconnessioni. Questa crescita interessa in modo estensivo le singole entità e i sistemi più complessi, con una amplificazione abnorme sia dei nodi che del numero delle entità elementari connesse.
Le reti telematiche e il world wide web rappresentano il fenomeno più evidente e conosciuto di questo processo anche se nei fatti la trama dei collegamenti rimanda a una realtà più complessa che riguarda in modo ben più sostanziale il nuovo modello di produzione di beni e servizi e di diffusione delle conoscenze. Questa trama di connessioni rende più sfumata per ogni istituzione la demarcazione tra ambiente interno e ambiente esterno coinvolgendo, attraverso i singoli nodi, anche le unità più periferiche del network globale.
Da questo punto di vista la rete informatica costituisce più propriamente la infrastruttura che permette la connessione di un sistema di relazioni immateriali ben più ampio della rete stessa, così come la rete dei trasporti determina le relazioni "fisiche" tra gli individui.

E' inevitabile che proprio per la sua rilevanza il cyberspazio[1], cioè il meta piano in cui tenderanno a

[1] "*Il termine cyberspazio apparve nel 1982, nella sua forma inglese cyberspace, in un racconto di fantascienza dal titolo Burning Chrome (1989), pubblicato da William Gibson sulla rivista Omni, per poi essere nuovamente utilizzato due anni dopo nel suo romanzo Neuromancer. Quest'ultimo lavoro di Gibson ebbe maggior fortuna, contribuendo in modo importante alla diffusione del termine, che deriva dalla fusione di «cibernetica» (parola coniata nel 1948 da Norbert Wiener per indicare i fenomeni biologici, artificiali o misti di*

concentrarsi sempre più le relazioni tra i sistemi e gli individui sia destinato a diventare un nuovo terreno in cui si trasferiscono fenomeni criminali consolidati nel piano reale delle relazioni economiche, politiche e sociali. Criminalità, terrorismo, spionaggio e scontro tra Stati hanno trasferito in questo spazio la loro azione secondo un processo di estensione "territoriale", occupando il nuovo terreno relazionale.

Se così fosse, se cioè gli episodi di cyber crime e di cyber attack contro gli individui, le imprese e le istituzioni fossero solo la manifestazione di un adattamento degli attori alla nuova realtà, il tema della cyber sicurezza si limiterebbe ad essere sul piano concettuale null'altro che l'adeguamento di processi di controllo e di contrasto ad un contesto operativo più complesso e dematerializzato.

Considerata però la rilevanza dei cambiamenti in atto è doveroso porsi una domanda sulla possibilità che questa estensione dell'ambito in cui si manifestano fenomeni criminosi sia in realtà espressione di una mutazione del connotato dei rischi delle singole azioni anomale. In concreto occorre stabilire in che modo le caratteristiche del mezzo in cui si svolgono le azioni rendano in qualche modo qualitativamente diverso il contenuto stesso delle fattispecie criminose[2].

Se così fosse, come peraltro siamo convinti che sia, avremmo bisogno di un nuovo paradigma per interpretare i rischi incombenti e dovremmo passare ad un diverso ordine di grandezza per misurare gli stessi.

La risposta affermativa a questo quesito viene suggerita dalla costatazione della portata del sistema di connessione. Come si intuisce, più sono le relazioni di un sistema, maggiori sono le possibilità di infezione. In questo senso la capacità intrinseca del network di diffondere situazioni di crisi va di pari passo con l'elaborazione di strategie che presentano un più elevato potere distruttivo.

In origine il tema della cyber sicurezza ha riguardato proprio il contrasto all'utilizzo delle reti come mezzo per ampliare la gamma degli strumenti disponibili per compiere attività di criminalità contro le aziende o gli Stati. Si pensi ad esempio al tema dello spionaggio industriale attuato attraverso l'intrusione e la manomissione di reti private e pubbliche che ha costituito un tema ricorrente di contrasto tra gli Stati Uniti e la Cina. La fase pioneristica del cyber crime è stata contrassegnata dal fenomeno della truffa perpetrata attraverso i mezzi messi a disposizione dal nuovo canale di comunicazione.

La novità del nuovo contesto consiste in un utilizzo più evoluto dei sistemi di connessione che vengono sfruttati per raggiungere obiettivi (ad esempio danneggiamento, operazioni di security, sabotaggi o furti) propriamente collegati al mezzo in quanto tale. In questo processo di trasformazione degli obiettivi e, attraverso l'uso di paradigmi di azione coerenti con lo sviluppo delle relazioni, è mutato anche la natura del rischio associato. Una mutazione che non riguarda tanto, o solo, l'aspetto quantitativo del rischio, quanto la configurazione e la caratterizzazione dello stesso. Il bisogno di adattamento degli strumenti al nuovo scenario riguarda tutti i campi ma, come spesso avviene, è il terreno politico militare a dover affrontare per primo le nuove minacce. In primo luogo si deve inquadrare il nuovo terreno di scontro dentro quelle che sono le tradizionali regole giuridiche e comportamentali che disciplinano i rapporti tra gli stati[3]. In

autoregolazione) e «spazio»" in Treccani, "Lessico del XXI secolo"

[2] "*The Internet has made the world a substantially smaller place and more connected in ways that were seemingly impossible before now. However, with all the positive things that exist thanks to the Internet and technology, there is also a sinister, unwholesome side that exists simultaneously. As in the physical world, the cyber world breeds criminals looking to make a quick buck through fraudulent means, hackers looking for fun, hacktivists looking to make a political or social point, terrorists looking to recruit new members, and finally, government organizations looking to advance their country's power or position in the global hierarchy. Individuals, states, and non-state actors use cyber-attacks as a way to advance their agenda. Common examples of cyberattacks include computer viruses, worms, malware, and distributed denial of service (DDoS) attacks*" Ken M. Jones (2015), "*Cyber war: the next frontier for NATO*", Naval Postgraduate School, Monterey, California

[3] Un interessante contributo per inquadrare la complessa materia è quello di Marco Roscini (2010), "*World wide warfare. Jus and bellum and the use of cyber force"*, in Von Bogdandy A. e Wolfrum R. (editors), "Max Planck Yearbook of United Nations law", Vol. 14, pagg 85-130

questo senso ha fatto storia la predisposizione del cosiddetto *Tallin Manual* che rappresenta un tentativo di ridefinire la legge internazionale in un contesto di cyber warfare. Il documento, sebbene non abbia alcuna ufficializzazione e ratifica da parte degli stati nazionali, è diventato il più influente punto di riferimento per definire le controversie legali che riguardano la materia[4].
Anche sul piano più prettamente operativo la situazione è destinata a subire una accelerazione. Fa testo l'avvio, il 20 aprile 2016, delle più grandi ed avanzate esercitazioni di cyber difesa a cui partecipano tutti i 19 paesi NATO. La simulazione prevede di testare la capacità di risposta ad un attacco al sistema informativo di un paese alleato[5].

Sarebbe comunque errato pensare che il tema della sicurezza informatica sia esclusivamente un tema militare. Questa affermazione non è vera in primo luogo con riferimento agli enti oggetto delle azioni di attacco che vengono frequentemente individuate seguendo un obiettivo industriale e economico. Allo stesso modo la creazione di un ambiente più sicuro passa necessariamente attraverso una collaborazione tra entità statali e private. Le pagine che seguono, con il racconto dei principali casi fino ad oggi conosciuti, mostrano in modo evidente il contributo delle società private specializzate nel contrasto alle azioni di sabotaggio. Molto spesso però queste attività di sorveglianza e di difesa si collocano in un terreno di frontiera dove la sicurezza nazionale si mischia in alcuni paesi con la questione della repressione del dissenso[6].

Questo ragionamento apre un nuovo filone di riflessione a dimostrazione di come lo sviluppo del cyber spazio modifichi in modo sostanziale il framework entro cui è stata fino ad ora risolta la distinzione di ciò che è lecito e ciò che illecito sia sul piano giuridico che su quello morale.
La questione più rilevante riguarda il diritto alla privacy, e i termini del dibattito sono arrivati al grande pubblico a seguito di alcuni recenti fatti di cronaca. Il più noto riguarda la richiesta di FBI alla Apple (9 febbraio 2016) di sboccare l'Iphone dell'attentatore di San Bernardino (California), responsabile dell'uccisione di 14 persone il 2 dicembre 2015. Il rifiuto della casa di Cupertino a collaborare con le autorità ha aperto una delicata controversia legale che si è conclusa solo dopo che l'FBI è riuscita autonomamente a raggiungere lo scopo di accedere ai dati contenuti nel cellulare.
Un secondo episodio è meno noto, ma è ancora più significativo sul piano delle conseguenze: la vicenda riguarda la decisione del 2 maggio 2016 di un giudice della corte locale dello stato brasiliano di Sergipe di bloccare per 72 ore i servizi di WhatsApp in tutto il paese[7] dopo il rifiuto dei responsabili della società a rendere noto il contenuto di alcune comunicazioni che sarebbero state utilizzate all'interno di un'indagine criminale.

Considerata la complessità e la vastità della materia affrontata in questo documento, il modo migliore per esaminare e comprendere il significato delle chiavi di lettura che vogliamo proporre è quello di ripercorrere sinteticamente i fatti emblematici che hanno contrassegnato la storia di questo nuovo rischio. Abbiamo scelto tra tutti gli episodi quelli che, in una moltitudine molto ampia, si sono caratterizzati per la loro maggiore potenziale valenza sistemica.

---

[4] Il Tallin Manual è stato redatto tra il 2009 e il 2012 da una ventina di esperti di diversi paesi su invito del Cooperative Cyber Defence Center della Nato. La prima versione del manuale è stata pubblicata nel 2013, mentre una seconda versione, *Tallin 2.0*, è stata rilasciata nel 2016.

[5] L'esercitazione, denominata Locked shield, coinvolge 550 esperti civili e militari impegnati nella simulazione di un attacco alle infrastrutture informative di un paese di fantasia, Berylia. Locked shield si sviluppa in uno scenario complesso che prevede, come nella realtà, la compresenza di una pluralità di strumenti, che vanno dalla rete di personal computer agli smartphone, e di più sistemi operativi, Windows, Linux e Apple IOS.

[6] Una bellissima, interessante e concreta ricostruzione dei termini del problema è contenuta in un lungo articolo di Foreign Policy che ricostruisce l'affermazione sul mercato della sicurezza delle imprese dell'Italiano David Vincenzetti.
David Kushner (2016), "*Fear This Man. To spies, David Vincenzetti is a salesman. To tyrants, he is a savior. How the Italian mogul built a hacking empire*", Foreign Policy, 26 aprile

[7] E' la seconda volta che un giudice brasiliano blocca l'attività del servizio di messaging. La prima volta risale al 15 dicembre 2015 ed era stata assunta da un giudice dello Stato di San Paolo che aveva sospeso il servizio per 48 ore.

Attacco all'Estonia

Il cyber attacco lanciato contro l'Estonia che ha prodotto il blocco completo della attività internet nel paese viene considerato come l'atto di nascita della cosiddetta cyber warfare. L'attacco degli hacker è iniziato il 27 aprile 2007 ed è stato risolto solo il successivo 18 maggio dopo che erano stati resi totalmente inoperativi tutti i siti governativi, quelli delle principali banche oltre agli account personali di migliaia di cittadini. Questa azione si è basata sulle tecniche cosiddette DDOS (Distributed denial of service) che prevedono l'indirizzamento di milioni di richieste a siti web fino a provocarne il collasso.
Le responsabilità dell'attacco sono state attribuite, anche in sede processuale, a hacker ispirati direttamente dalle autorità russe. In quei giorni era in corso una disputa dalla forte valenza simbolica riferita la rimozione da una piazza di Tallinn di una statua dedicata ai soldati sovietici. Per estoni e russi la vicenda è diventata il pretesto per rinfocolare la storica opposizione tra la nuova Repubblica del Baltico e quella che viene considerata dagli estoni la potenza che ha invaso e sottomesso il paese per decenni.
La novità e la portata di questa operazione contro uno stato sovrano ha avuto vasta eco determinando un ripensamento strategico, anche sul piano delle dottrine militari, di quelli che sono i rischi che derivano da azioni condotte attraverso la rete[8].

Un attacco analogo si è registrato nelle settimane cha hanno preceduto il breve conflitto tra Russia e Georgia[9].

Ripetuto in Georgia. Il primo episodio di questa campagna informatica si è avuto il 20 luglio 2008, con l'attacco di un gruppo di hacker al sito del presidente georgiano Mikheil Saakashvili[10]. A seguire, con cadenza quasi giornaliera, sono stati presi di mira decine di istituzioni pubbliche e private.

Stuxnet: attacco al programma nucleare

Il caso, però, che più di tutti gli altri segna il passaggio alla nuova fase vede come protagonista il paese che da allora è diventato uno dei principali attori del cosiddetto cyber terrorismo. In questo caso l'Iran ha ricoperto il ruolo di vittima di un attacco informatico che ha avuto come obiettivo le infrastrutture del programma nucleare. Eravamo nel pieno dell'emergenza che ha portato Israele e suoi alleati occidentali sull'orlo della guerra: l'avanzamento del programma nucleare di Teheran giunto a un passo dalla produzione di un ordigno nucleare. Con questo caso per la prima volta la cyber warfare entra in una nuova fase: non siamo di fronte ad un atto di puro sabotaggio quanto piuttosto ad un sofisticato uso di strumenti atti a manipolare sistemi nevralgici per la sicurezza nazionale.
Il malware utilizzato, che sfruttava alcuni buchi del sistema operativo Windows, si è introdotto nei sistemi di automazione che regolano il funzionamento delle centrifughe utilizzate per l'arricchimento dell'uranio.
L'infezione è stata scoperta e denunciata da una società che si occupa di sicurezza informatica nel giugno del 2010[11] dopo che per un errore il virus si è propagato indiscriminatamente dai sistemi dell'impianto di arricchimento nucleare di Natanz a migliaia di altri computer[12].

[8] Ad esempio le analisi che sono state condotte sulla vicenda Estone e il dibattito che ne è seguito hanno portato la NATO a defiire una propria strategia d'azione e a creare, nel maggio 2008, un Cooperative Centre of Excellence for Cyber Defense (CCDCOE), che ha sede proprio a Tallinn, oltre a una Cyber Defence Management Authority.
Sito ufficiale https://ccdcoe.org/

[9] Il conflitto armato è stato causato dalla proclamazione dell'indipendenza di due regioni georgiane, l'Abkhazia e l'Ossezia del Sud in vista di un loro avvicinamento a Mosca. Tiblisi aveva reagito con un'offensiva militare contro i ribelli iniziata il 7 agosto 2008. La Russia ne aveva approfittato per intervenire in difesa delle repubbliche ribelli con un'azione coordinata da terra e via mare che ha preso il via l'8 agosto. Di fronte alla sproporzione delle forze in campo la Georgia fu costretta a negoziare un cessate il fuoco il 12 agosto.

[10] Anche in questo caso l'attacco è stato condotto con l'invio di milioni di messaggi (DDOS) contenenti la frase "win+love+in+Rusia".

[11] In realtà la prima versione del malware è stata diffusa probabilmente un anno prima, nel giugno del 2009. Una ricostruzione dettagliata dell'intero caso è contenuta in Kim Zetter (2014), "*Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*"

[12] Un rapporto di Symantec, una delle società leader del settore della sicurezza informatica, spiega come gli attacchi mirati a singoli obiettivi siano destinati a produrre effetti collaterali su vasta scala.

Sebbene l'attacco non sia mai stato rivendicato, un articolo del New York Times del 15 gennaio 2011 fornisce le prove della collaborazione tra gli Stati Uniti e Israele nello sviluppo del malware "Stuxnet worm"[13].

Operazione Abadil

L'Iran è forse il paese che ha più compreso le "opportunità" di sfruttare a proprio favore le nuove frontiere della cyber guerra, trasformandosi rapidamente da soggetto passivo degli attacchi in uno dei principali attori della guerra cibernetica.

L'operazione Abadil è stata lanciata da un gruppo di hacker, conosciuti come Qassam Cyber Fighters, a partire dal 18 settembre 2012. Secondo i comunicati diffusi via web l'obiettivo dell'attacco era quello di ottenere la rimozione da internet del film *Innocence of Muslims*, considerato antiislamico e la cui produzione aveva scatenato ondate di proteste in tutto il mondo arabo[14].
I target dell'attacco sono state 46 istituzioni finanziarie tra cui la New York Stock Exchange, J.P. Morgan Chase e Bank of America[15]. L'attacco si è concluso nella sua prima fase il 23 ottobre del 2012[16].
L'offensiva contro le istituzioni economiche si è compiuta indirizzando volumi di traffico abnormi verso i server delle società target al fine di far collassare l'intero sistema.
Secondo una denuncia del senatore Joseph Lieberman presidente della Commissione Homeland Security and Governmental Affairs del Senato USA e rilanciata dal Washington Post[17], l'attacco sarebbe stato in realtà realizzato direttamente dalle milizie Quds, un braccio speciale dei Guardiani della rivoluzione iraniana, con il vero obiettivo di rispondere alle sanzioni economiche che i paesi occidentali avevano varato come ritorsione contro il programma di riarmo nucleare.

Operazione Cleaver

Un'altra azione che attesta il ruolo crescente dell'Iran nella cyber warfare è conosciuta come operazione Cleaver.
La notizia dell'attacco cibernetico che ha colpito una cinquantina di imprese in 16 paesi diversi[18], è stata resa noto in un rapporto redatto nel dicembre del 2014 dalla società di sicurezza Cylance Inc[19]. Secondo il rapporto, le

"*The primary purpose of the Stuxnet worm is to take control of industrial facilities. Interestingly, one would expect the malware authors to design malware that would target only computers running the software that controls these facilities. However, like any other garden variety worm, it spreads indiscriminately using the vulnerability mentioned above.*"
https://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99

[13] Secondo le fonti del giornale lo sviluppo è partito nel 2008 quando la Siemens, produttrice dei sistemi informatici oggetto dell'attacco, e l'Idaho National Laboratory, l'istituto governativo responabili per i test sui reattori nucleari, hanno collaborato per individuare eventuali vulnerabilità dei sistemi di controllo informatici.

[14] Le proteste erano già iniziate il 2 luglio 2012 quando il trailer del film era stato pubblicato su Youtube. Prodotto da uno scrittore egiziano cristiano residente negli Stati Uniti, il film era stato promosso dal controverso pastore americano Terry Jones salito alle cronache per la sua iniziativa di bruciare pubblicamente copie del Corano.

[15] In realtà l'attacco si è protratto per molti mesi attraverso quattro fasi distinte protrattesi fino all'estate del 2013. Una ricostruzione dell'intera vicenda è contenuta in:
https://conference.apnic.net/data/37/breakingthebank.pdf

[16] Redware, una società israeliana specializzata nel settore sicurezza, ha ricostruito la sequenza degli attacchi.
18 settembre 2012 - Bank of America, New York Stock Exchange e JPMorgan Chase
25 settembre 2012 - Wells Fargo, U.S. Bank
27 settembre 2012 - PNC Bank
9 ottobre 2012 - Capital One Financial Corp.
10 ottobre 2012 - SunTrust Banks
11 ottobre 2012 - Regions Financial Corp.
16 ottobre 2012 - The Capital One Financial Corp.
17 ottobre 2012 - BB&T Corp.
18 ottobre 2012 - HSBC Bank USA

[17] Nakashima Ellen (2012), "*Iran blamed for cyberattacks on U.S. banks and companies*", in The Washington Post,21 settembre

[18] Alcuni nomi che sono trapelati sono quelli di Calpine Corp, società energetica californiana, Aramco, della società petrolifera di stato dell'Arabia Saudita, della messicana Petroleos Mexicanos, della Qatar Airlines e di Korean Air.

[19] Cylance, "#OPCleaver",

indagini degli esperti della società durate due anni hanno fatto emergere un legame degli attacchi con le Guardie rivoluzionarie iraniane. Le accuse sono state però rigettate dalle autorità di Teheran; il portavoce della missione iraniana alle Nazioni Unite ha dichiarato che: "*Cylance's report as a baseless and unfounded allegation fabricated to tarnish the Iranian government image, particularly aimed at hampering current nuclear talks*."
Le imprese target operano tutte in diversi settori strategici: petrolio e gas naturale, energetico, aeroporti, telecomunicazioni, agenzie governative.
Secondo il rapporto l'azione non era mirata al furto di dati e segreti industriali ma si è concentrata nel raccogliere informazioni sulla strutturazione dei network e sul loro funzionamento oltre che su altre informazioni sensibili, acquisendo via via un controllo su parti critiche delle reti. L'operazione Cleaver rappresenta quindi un salto di qualità segnando il passaggio da pure azioni di sabotaggio a obiettivi più complessi che mirano, come è stato per Stuxnet, al controllo e alla manipolazione dei sistemi informativi di imprese e istituzioni strategiche.

Le superpotenze della cyber warfare

Le superpotenze che dominano il nuovo campo di battaglia sono gli Stati Uniti, il Regno Unito, Israele, Russia e Cina.
La Cina costituisce l'esempio tipico di una minaccia soprattutto nel campo dello spionaggio militare e civile. Durante una visita ufficiale negli Stati Uniti il Presidente Cinese Xi Jinping ha dovuto implicitamente fornire rassicurazioni alla comunità internazionale rispetto al ruolo della Cina soprattutto nel campo dello spionaggio industriale, "*The Chinese government will not in whatever form engage in commercial theft, and hacking against government networks are crimes that must be punished in accordance with the law and relevant international treaties*"[20] Malgrado queste assicurazioni non sembra, almeno dalle accuse che vengono confermate dagli ambienti della sicurezza, che gli attacchi siano diminuiti.

Con un documento rilasciato l'11 maggio 2016 l'FBI[21] ha inteso mettere in guardia le imprese e le istituzioni circa la persistente e crescente minaccia informatica[22]

Sul piano invece di una strategia più complessa opera l'Iran che, come abbiamo già avuto modo di rilevare, si sta affermando come nuova potenza informatica.
A questo proposito è interessante richiamare altri episodi che hanno segnato l'escalation iraniana:

- ✓ Intrusione nei sistemi di Comodo, società britannica specializzata nell'emissione di certificati di sicurezza. La società, il 23 marzo 2011, dichiara di aver subito un attacco ai propri sistemi, iniziato 8 giorni prima, che ha comportato la sottrazione di diverse credenziali. Le successive verifiche hanno evidenziato come l'attacco sia partito dall'Iran.
- ✓ DigiNotar. La società danese era specializzata nell'emissione di certificati di sicurezza ed ha subito un'intrusione nel sistema. Gli hacker hanno prodotto decine di migliaia di falsi certificati che sono stati utilizzati per ulteriori operazioni di hackeraggio. La società è fallita in conseguenza dei danni economici e reputazionali seguiti all'attacco.
- ✓ Sabotaggio alla compagnia petrolifera Saudita Aramco, utilizzando il malware Shamoon, capace di distruggere il contenuto dei sistemi informatici. L'attacco è stato lanciato il 15 agosto 2012 e ha infettato 30 mila computer della rete interna della compagnia[23].
- ✓ Intrusione nel sistema della rete Navy Marine Corps Intranet (2013) che ha permesso agli iraniani di muoversi indisturbati per quattro mesi nei sistemi della marina statunitense.

https://cdn2.hubspot.net/hubfs/270968/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf

[20] Perlez Jane (2015), "*Xi Jinping Pledges to Work With U.S. to Stop Cybercrimes*" in The New York Times, 22 settembre

[21] L'FBI ha costituito un centro di commando Cyber Watch (CyWatch) per monitorare e prevenire le azioni di intrusioni informatica nei sistemi e per coordinare le risposte adeguate. https://www.dsac.gov/topics/cyber-resources

[22] Il documento è reperibile su internet http://freebeacon.com/wp-content/uploads/2016/05/FLASH-E-000072-MW.pdf

[23] https://www.iiss.org/en/publications/survival/sections/2013-94b0/survival--global-politics-and-strategy-april-may-2013-b2cc/55-2-08-bronk-and-tikk-ringas-e272

- ✓ Operation Saffron Rose, con cui un gruppo di hacker iraniani ha preso di mira imprese collegate al sistema di difesa statunitense. Iniziata nell'ottobre del 2013 è proseguita fino all'aprile dell'anno successivo[24].
- ✓ Operazione Newcastle, operazione di spionaggio che, a partire dal 2011 fino al momento della sua scoperta nel 2014, ha avuto come target persone che ricoprono incarichi critici negli Stati Uniti, in Israele, Gran Bretagna, Arabia Saudita, e in altri paesi[25].

L'importanza di acquisire un ruolo di preminenza nel cyber spazio viene ripetutamente affermata ai massimi livelli del potere di Teheran. Il Leader Supremo della Rivoluzione islamica, l'Ayatollah Ali Khamenei, presenziando ad una riunione del Supremo Consiglio per il Cyberspazio ha evidenziato il compito strategico affidato all'istituzione pubblica: "*Using capability and talents of the country's youth and through making right policies and adopting well-calculated and coordinated measures and without losing time, let's move towards ridding the cyberspace of passivity and having active, influential presence and production of reliable and attractive Islamic content*"[26].
Oltre ad agire contro gli altri paesi il Supremo Consiglio per il Cyberspazio svolge anche una funzione di controllo interno e di repressione delle voci critiche. Ad esempio durante le ultime elezioni il Governo ha deciso di monitorare l'attività che si svolgeva nei social media riguardante il dibattito sui temi elettorali[27].

Anche paesi minori come la Corea del Nord si sono strutturate per condurre questo nuovo tipo di guerra. L'esercito di Pyongyang ha creato al proprio interno una divisione, conosciuta con il nome di Bureau 121, per la gestione della cyber warfare[28].

Attacco alla Sony

La scoperta dell'azione di hackeraggio avviene il 24 novembre 2014 quando il malware installato blocca numerosi computer della Sony producendo sugli schermi un messaggio di rivendicazione firmato da sedicenti "Guardians of Peace". Contestualmente inizia la pubblicazione su web di una serie di informazioni riservate che erano state sottratte per circa un anno dai server. Le informazioni riguardavano l'attività della Sony e dei suoi collaboratori, numerose comunicazioni personali dei suoi dipendenti e delle star che lavorano per la società, nonché progetti dettagliati sui futuri film e progetti di sviluppo[29] .

Le agenzie investigative hanno attribuito la responsabilità del crimine direttamente al Governo della Corea del Nord. In particolare l'FBI ha pubblicato un comunicato il 19 dicembre 2014 che accusa lo stato asiatico sulla base della comparazione delle tecniche simili rispetto ad altre di precedenti attacchi sicuramente riconducibili a Pyongyang.

---

[24] La minaccia è stata rivelata dalla società di sicurezza californiana FireEye che ha rilasciato un dettagliato rapporto il 13 maggio 2014.
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf

[25] La società di cyber sicurezza texana iSIGHT Partners il 29 maggio 2014 pubblica un rapporto che denuncia l'attività di spionaggio in corso. Secondo il rapporto il gruppo di hacker ha usato "*a combination of fake login pages, phishing emails and custom-built malware to steal login credentials and other data. In one attack, the group targeted US-based aerospace companies by creating a fake registration page for the 2014 IEEE Aerospace conference*."
https://www.isightpartners.com/2014/05/newscaster-iranian-threat-inside-social-media/

[26] The Iran Project (2015), "*Supreme Leader urges dynamic presence in cyberspace*", 7 settembre

[27] Karami Arash (2015) "*Iran's Supreme Council of Cyberspace announces plans for social media monitoring*", in Al Monitor, 23 febbraio.

[28] Come per tutte le questioni che riguardano i temi interni della Corea del Nord circolano diverse voci, alcune decisamente favolistiche, sulla reale consistenza ed efficacia di queste strutture. Secondo alcuni osservatori il Bureau conta addirittura 1.800 specialisti, scelti tra i laureati della facoltà di Automazione dell'Università della capitale.

[29] La Sony era stata già oggetto di un attacco informatico nel 2011 (tra il 17 e il 19 aprile) quando era stato bucato il sistema di sicurezza del network della popolare piattaforma di videogiochi Playstation, con la sottrazione di circa 77 milioni di account. L'attacco ha costretto gli amministratori a bloccare per 23 giorni il sistema.

Peraltro i Guardiani della Pace nella loro rivendicazione hanno fatto esplicito riferimento alla produzione di un film della Sony, "The interview", che racconta l'assassinio del presidente nord coreano. Il gruppo di hacker ha minacciato anche alcuni attentati terroristici nelle sale dove sarebbe stata proiettato il film. La Nord Corea aveva già cercato di bloccare l'uscita della pellicola accusandola "*di costituire una esplicita incitazione alla violenza e al terrorismo*"
L'azione ha raggiunto i suoi obiettivi dal momento che Sony ha deciso di ritirare il film da tutte le sale passando direttamente alla distribuzione digitale.
Sony ha subito parecchi danni diretti e indiretti da questa azione. Sul piano reputazionale la società ha dovuto subire per mesi i contraccolpi della pubblicazione delle informazioni riservate. Solamente Wikileaks di Julian Assange ha pubblicato nel mese di aprile 2015 oltre 30 mila file riservati. Sony si è dovuta impegnare in una costosa battaglia legale per impedire la pubblicazione sui vari social del materiale riservato. Inoltre Sony Pictures Entertainment ha dovuto fare i conti con una causa collettiva di ex dipendenti con l'accusa di non aver protetto adeguatamente i dati sensibili, comprese le informazioni sulla salute dei dipendenti e i numeri personali della Sicurezza sociale.

Al di là del peso del caso specifico, enormemente amplificato dal peso mediatico dei soggetti coinvolti, l'importanza di questo caso deriva soprattutto dalla prova di vulnerabilità[30] di una delle principali corporazioni degli Stati Uniti e dalle conseguenze politiche del caso. Sebbene la Corea del Nord si sia sempre dichiarata estranea al sabotaggio è risultato sconcertante come un piccolo paese, nemmeno particolarmente evoluto sul piano tecnologico, abbia potuto attaccare con successo una delle più importanti major americane.
Sotto accusa è stata posta l'incapacità del governo americano di proteggere gli interessi delle principali società del paese anche attraverso una maggiore collaborazione nel campo della sicurezza. Il 10 febbraio 2015 il Presidente Obama, sotto la spinta di crescenti critiche, annuncia la creazione di una nuova agenzia, il *Cyber Threat Intelligence Center*, per coordinare gli sforzi di prevenzione contro gli attacchi cibernetici.

Per gli aspetti specifici la vicenda si colloca a cavallo tra quelle che sono le tradizionali minacce alla sicurezza delle imprese e agli Stati e la nuova stagione di impiego degli strumenti informatici per fini politici.

Il furto ai danni della Banca Centrale del Bangladesh

Sicuramente una scarsa attenzione al tema della vulnerabilità ha premesso il verificarsi del caso più eclatante di *cyber crime*. L'episodio si è verificato nei primi mesi del 2016 a danno della Banca Centrale del Bangladesh. I protagonisti della vicenda sono, oltre al gruppo di hacker che ha compiuto il colpo, la Banca Centrale del paese asiatico, la Federal Reserve di New York e il consorzio interbancario SWIFT[31].
Secondo le ammissioni dei vari protagonisti la truffa si è potuta realizzare grazie all'inserimento di un malware nel sistema informatico di SWIFT (Society for Worldwide Interbank Financial Telecommunication), il consorzio tra istituti finanziari che garantisce a livello globale le transazioni di denaro tra le banche, circa 11 mila, con sede in oltre 200 paesi.
Il malware è stato istallato all'interno del cuore del sistema, denominato Alliance Access (AA) che, come riportato nel sito ufficiale del consorzio, rappresenta "*SWIFT's market leading messaging interface, allows banks and market infrastructures to connect to SWIFT*".
A cavallo tra il 4 e il 5 febbraio 2016, sfruttando la falla creata nel sistema SWIFT gli hacker hanno iniziato a ordinare trasferimenti dal conto della Banca Centrale del Bangladesh aperto presso la Federal Reserve di New York. Il malware è stato programmato per compromettere le transazioni sul client AA consentendo il prelievo di

[30] I buchi che si possono creare nei sistemi informativi e nelle reti hanno dato luogo alla necessità di sviluppare specifiche competenze nell'ambito dell'enterprise risk managment volte al cosiddetto vulnerability management, cioè alla identificazione e alla gestione dei punti deboli di un sistema complesso.

[31] SWIFT ha sede a Bruxelles e garantisce il funzionamento di un network che rende possibile in modo efficiente, tempestivo e sicuro le transazioni monetarie tra istituzioni finanziarie. I protocolli di comunicazione e le sintassi utilizzate da SWIFT rappresentano oggi lo standard internazionale. Informazioni dettagliate sono reperibili sul sito ufficiale www.swift.com.

fondi e al tempo stesso coprendo le tracce delle operazioni con messaggi e report falsi inviati agli operatori bancari coinvolti. Utilizzando le credenziali rubate gli hacker hanno richiesto decine di movimenti verso entità delle Filippine e dello Sri Lanka.
Con i primi quattro ordini sono stati sottratti 81 milioni di dollari. Al quinto passaggio il meccanismo si è inceppato per un errore banale. L'ordine di trasferimento prevedeva come destinatario una presunta fondazione umanitaria con sede nello Sri Lanka. Un banale errore di indicazione del beneficiario dell'ordine di 20 milioni, "Shalika Fandation", anziché "Shalika Foundation" ha destato i sospetti consentendo di bloccare gli ordini in coda di esecuzione che avrebbero svuotato interamente il deposito di 950 milioni di dollari presenti sul conto.
Al di là della sofisticazione della truffa e dell'entità della somma di denaro sottratta questo caso assume un rilievo in funzione dello standing dei soggetti coinvolti. In particolare il coinvolgimento del consorzio SWIFT e la vulnerabilità mostrata dal sistema assume una rilevanza sistemica nella misura in cui ha interessato l'infrastruttura che garantisce gli scambi di denaro a livello planetario. Secondo quanto riportato da Reuters SWIFT ha dovuto ammettere con un comunicato interno inviato il 25 aprile a tutti i suoi utilizzatori che "*the Bangladesh Bank attack was not an isolated incident but one of several recent criminal schemes that aimed to take advantage of the global messaging platform used by some 11,000 financial institutions*."
Il caso costituisce peraltro un classico esempio di evento di coda che ha potuto verificarsi grazie ai buchi che rimangono nell'operatività dei sistemi complessi. Le verifiche ex post hanno potuto accertare che la Banca Centrale del Bangladesh disponeva di misure di sicurezza insufficienti e le transazioni erano affidate a switch di rete di seconda mano (dal valore di 10 dollari ciascuno) e da nessun firewall[32]. Anche lo stesso malware che è stato utilizzato "evtdiag.exe" risulta abbastanza comune. Secondo il sito specializzato Payload Security il malware "*was identified as malicious by a large number of Antivirus engines*"[33].
Il Financial Times ha riportato la dichiarazione dell'amministratore delegato di Swift secondo cui il consorzio sarebbe intenzionato di escludere dal network quelle realtà bancarie che non sono in grado di assicurare un livello di sicurezza adeguato[34].
Allo stesso tempo le autorità del Bangladesh hanno accusato la Fed di carenza nei sistemi di controllo dal momento che ha autorizzato trasferimenti di tale portata non a favore di un'istituzione finanziaria ma a soggetti estranei al circuito che non erano peraltro mai stati destinatari di precedenti disposizioni. Diversi specialisti della sicurezza informatica hanno stigmatizzato l'assenza di alert automatici in grado di segnalare il verificarsi di operazioni anomale.
Complessivamente pertanto il caso evidenzia un complessivo fallimento di tutta la catena di controlli in soggetti istituzionali deputati tra l'altro a presidiare il rispetto del monitoraggio dei rischi operativi presso i soggetti vigilati. Colpiscono tra l'altro le dichiarazioni rilasciate il 15 marzo 2016 dal presidente della Banca Centrale del Bangladesh, Atiur Rahman, in cui si afferma che gli uffici competenti lo hanno informato solo dopo un mese che si è verificato il furto e in coincidenza delle prime indiscrezioni apparse sui media.

In realtà il furto a danno della Banca del Bangladesh non sembra essere un caso isolato. Recentemente il deposito della documentazione inerente una causa contro la banca statunitense Wells Fargo (28 gennaio 2016), accusata di mancati controlli, ha fatto emergere l'attacco, fino ad allora tenuto segreto, contro un istituto equadoriano, Banco del Austro risalente al gennaio

[32] Per leggere una descrizione di come ha funzionato la truffa sul piano informatico si rimanda al documento tecnico pubblicato sul sito di Bae Systems, Sergei Shevchenko (2016), "*Two bites to $951M*", 25 aprile
http://baesystemsai.blogspot.it/2016/04/two-bytes-to-951m.html

[33] Sempre secondo il sito il malware viene identificato da 14 dei 56 prodotti analizzati dal campione di mercato monitorato dalla società.

[34] Arnold Martin (2016), "*Swift warns bank over security*", 3 giugno
Secondo Gottfried Leibbrandt, CEO di Swift, "*The days when you need to break into a bank and carry guns and blow torches are over. You can now rob a bank from just own PC and that does change the game completely*", ibidem.pag. 13

2015[35]. Anche in questo caso l'utilizzo di credenziali del sistema Swift ha permesso agli hackers di trasferire 12 milioni di dollari dai conti del Banco a entità in Hong Kong, Dubai, New York e Los Angeles.
Anzi, la falla venutasi a creare nel sistema Swift sembra aver generato una proliferazione di attacchi secondo lo stesso modus operandi. Il 15 maggio 2016 la banca vietnamita Tien Phong Bank ha annunciato di aver sventato un tentativo di sottrazione di denaro dai propri conti messa a punto da hackers attraverso le credenziali Swift.

Nuovi territori da esplorare, nuovi campi di battaglia

La carrellata non potrebbe essere completa senza che vengano esaminati altri filoni in cui si sta combattendo la battaglia della cyber sicurezza.
Il primo esempio che vogliamo riportare si inquadra come episodio rappresentativo di come l'evoluzione delle strategie criminali sperimenti sempre nuove opportunità. Il caso riguarda denuncia fatta dal sito specializzato BusinessInsider e riguarda i dipendenti della filiale irlandese della Apple.
Secondo il sito di news, alcuni hacker avrebbero avvicinato e offerto a diversi dipendenti della casa della mela migliaia di Euro per ottenere le credenziali di login aziendali[36].

Il secondo esempio riguarda la sfera politica e ha avuto come epicentro Honk Kong durante la battaglia di migliaia di attivisti impegnati nella campagna "Occupy Honk Kong" contro le pretese avanzate da Pechino di porre fine all'autonomia amministrativa dell'ex città stato.

Oltre che nelle strade e nelle piazze la battaglia si è e si sta combattendo da entrambe le parti con un inedito dispendio di iniziative nel cyber spazio[37].

C'è infine il tema del cyber terrorismo. Ad esempio l'ISIS si è dotata di una propria struttura operativa conosciuta come Caliphate Cyber Army, che si è distinta per una serie di azioni a danno dei paesi occidentali. Ad esempio, dopo alcune intrusioni nei sistemi informatici di agenzie e istituzioni pubbliche statunitensi, il CCA ha postato i nomi e gli indirizzi di diversi funzionari incoraggiando i propri seguaci a colpirli.
Peraltro oltre ai costi economici questi attacchi terroristici possono creare enormi danni sia all'ambiente che alle persone. Secondo Ludolf Luehmann, IT manager della Shell "*It will cost lives and it will cost production, it will cost money, cause fires and cause loss of containment, environmental damage - huge, huge damage*."[38]

I costi: un nuovo onere per le imprese

Al di là di tutte le considerazioni relative alla rilevanza strategica della cyber sicurezza, una delle questioni più importanti da esaminare riguarda il tema dei costi che le imprese subiscono in caso di cyber attack.
Quando una società subisce un attacco informatico la stessa deve supportare in prima battuta gli effetti della interruzione della business continuity. Secondo Kaspersky Lab, una delle principali società del comparto sicurezza, in media un'impresa subisce un'interruzione

[35] Secondo la ricostruzione il 12 gennaio 2015 Wells Fargo ha ricevuto un'istruzione di trasferimento di denaro dal conto del Banco del Austro (BDA), a cui hanno fatto seguito altre richieste nei successivi 10 giorni.
Per una più ampia descrizione della vicenda si veda Bergin Tom e Layne Nathan (2016), "*Special Report: Cyber thieves exploit banks' faith in SWIFT transfer network*", Reuters, 20 maggio

[36] Sam Shead (2016), "*Hackers are offering Apple employees in Ireland up to €20,000 for their login details*" in BusinessInsider, 9 febbraio

[37] A questa vicenda un gruppo di ricercatori ha dedicato un capitolo di un libro in cui si analizzano le tecniche utilizzate e la strumentazione messa in campo, Kam-Pui Chow, Ken Yau, Frankie Li (2015), "*Cyber Attacks and Political Events: The Case of the Occupy Central Campaign*", in AAVV, "*IFIP Advances in Information and Communication Technology*".
Secondo lo studio, ad esempio, gruppi di hacker pro Pechino hanno istallato programmi spia sugli smartphone e sui computer dei manifestanti distribuendo il malware attraverso diversi canali compresa la messaggistica WhatsApp. La rete di Next Media, di proprietà dell'imprenditore Jimmy Lai Chee-ying, che si è schierato con la protesta, è stata oggetto di un attacco volto a paralizzarne l'operatività coinvolgendo circa 10,000 computer sparsi in tutto il mondo. Dall'altra parte la rete di Anonymous ha preso di mira oltre 70 siti governativi.

[38] BBC News (2012), "*Oil cyber-attacks could cost lives, Shell warns*", 8 marzo

delle proprie attività per almeno 23 ore con una perdita media di 1,4 milioni di dollari[39]

A questo onere si aggiunge un costo diretto di ripristino del sistema. Infine si devono aggiungere i costi, talvolta decisamente superiori, determinati dal danno reputazionale, oltre ad un'altra serie di costi indiretti[40].

Uno studio condotto nel 2014 da Oxford Economics in collaborazione con il Centre for the Protection of National Infrastructure su un campione di imprese britanniche arriva a stime di costo superiori, pari a 2,9 milioni di sterline[41]. Altri dati raccolti dall'indagine sono ancora più significativi sul piano qualitativo. Ad esempio il 61% delle imprese colpite da un cyber attacco ha dichiarato di avere subito una perdita sul piano competitivo. Altrettanto impressionante è la percentuale delle imprese che sono state colpite da un attacco, il 60% del campione. Bisogna peraltro tener conto del fatto che questi dati si riferiscono al 2014 e che i fenomeni che stiamo descrivendo stanno conoscendo una crescita esponenziale. Bisogna peraltro considerare che i resoconti ufficiali che danno conto dei danni subiti forniscono spesso valori inferiori alla realtà a causa della ritrosia delle imprese a fornire informazioni che possono avere una ripercussione negativa sulla reputazione del brand.

Per fare un esempio concreto il gruppo britannico di telecomunicazioni TalkTalk ha subito nell'ottobre 2015 un attacco informatico ai propri sistemi che, seppure intercettato nella sua fase iniziale, ha comportato la compromissione delle informazioni sui numeri delle carte di credito dei clienti e la sottrazione di altri dati personali degli utenti.

A causa dell'attacco TalkTalk ha dichiarato di aver perso circa 101.000 clienti (3% del totale) con un costo complessivo di ripristino della sicurezza pari a circa 80 milioni di sterline[42].

Oltre che sul piano della singola azienda la presenza di minacce concrete al business è destinata a produrre una lievitazione dei costi a livello di sistema. L'esigenza di dotarsi di protocolli di difesa sempre aggiornati e via via più complessi comporta la destinazione di risorse crescenti in questa area di copertura dei rischi. L'amministratore delegato di IBM, la signora Ginni Rometty, ha definito il cybercrime la più grande minaccia per le imprese a livello globale[43].

Il costo globale per le imprese di questi attacchi è enorme ed è stato stimato da una ricerca condotta dalla società di sicurezza McAfee in collaborazione con il Center for Strategic and International Studies[44] in un range compreso tra i 375 e 575 miliardi di dollari all'anno. Questi valori sono destinati anch'essi a crescere. Secondo Jupiter Research, una società di ricerca economica specializzata nel settore IT, nel 2019, il cyber crime costerà alle imprese 2.100 miliardi di dollari, un valore quasi pari al PIL dell'Italia, quadruplicando i valori rispetto al 2015. A questi numeri andrebbero aggiunti i danni provocati dallo spionaggio industriale che spesso viene scoperto solo dopo tempo e che produce un danno competitivo enorme alle imprese.

---

[39] Kenny Jake (2016), "*The True Costs of a Cyberattack for Enterprises", Kaspersky Lab*" 16 febbraio

[40] E' interessante peraltro notare la crescita di attenzione dei media per gli episodi di cyber attack che comporta di fatto una amplificazione dell'effetto mediatico e quindi del danno reputazionale. Il Rapporto annuale "*2015 Information security breaches survey*" commissionato dal Governo inglese e realizzato a partire dai primi anni novanta da PWC e Inforsecurity fotografa questa evoluzione.
Nel 2013 il 2% dei casi aveva avuto una "*Extensive adverse media coverage over a prolonged period*", mentre l'8% dei casi aveva subito una "*Some adverse media coverage*". Questi numeri sono saliti rispettivamente all'11 e 7% nel 2014 e al 17% e 17% nel 2015.

[41] "*Loss estimates were highest for damage to reputation / branding. All other costs were reported with raw averages around the £2 million mark, with adjusted means slightly under half that and medians of £175,000. However, the raw average reputation/branding loss estimate was £2.9 million.",* Oxford Economics (2014), "Cyber-attacks: Effects on UK Companies", Luglio

[42] Holton Kate e Weir Keith (2016), "*TalkTalk lost more than 100,000 customers after cyber attack*", Reuters, 2 febbraio

[43] Morgan Steve (2015), "*IBM's CEO On Hackers: 'Cyber Crime Is The Greatest Threat To Every Company In The World*", in Forbes, 24 novembre

[44] McAfee e Center for Strategic and International Studies (2014), "*Net Losses: Estimating the Global Cost of Cybercrime*", luglio

Una minaccia crescente

Possiamo concordare sul fatto che le minacce che si muovono nel cyber spazio sono in continua espansione. Questo fenomeno riguarderà il numero degli episodi ai quali i sistemi di sicurezza dovranno far fronte, ma soprattutto interesserà l'intensità con cui gli stessi si manifesteranno.

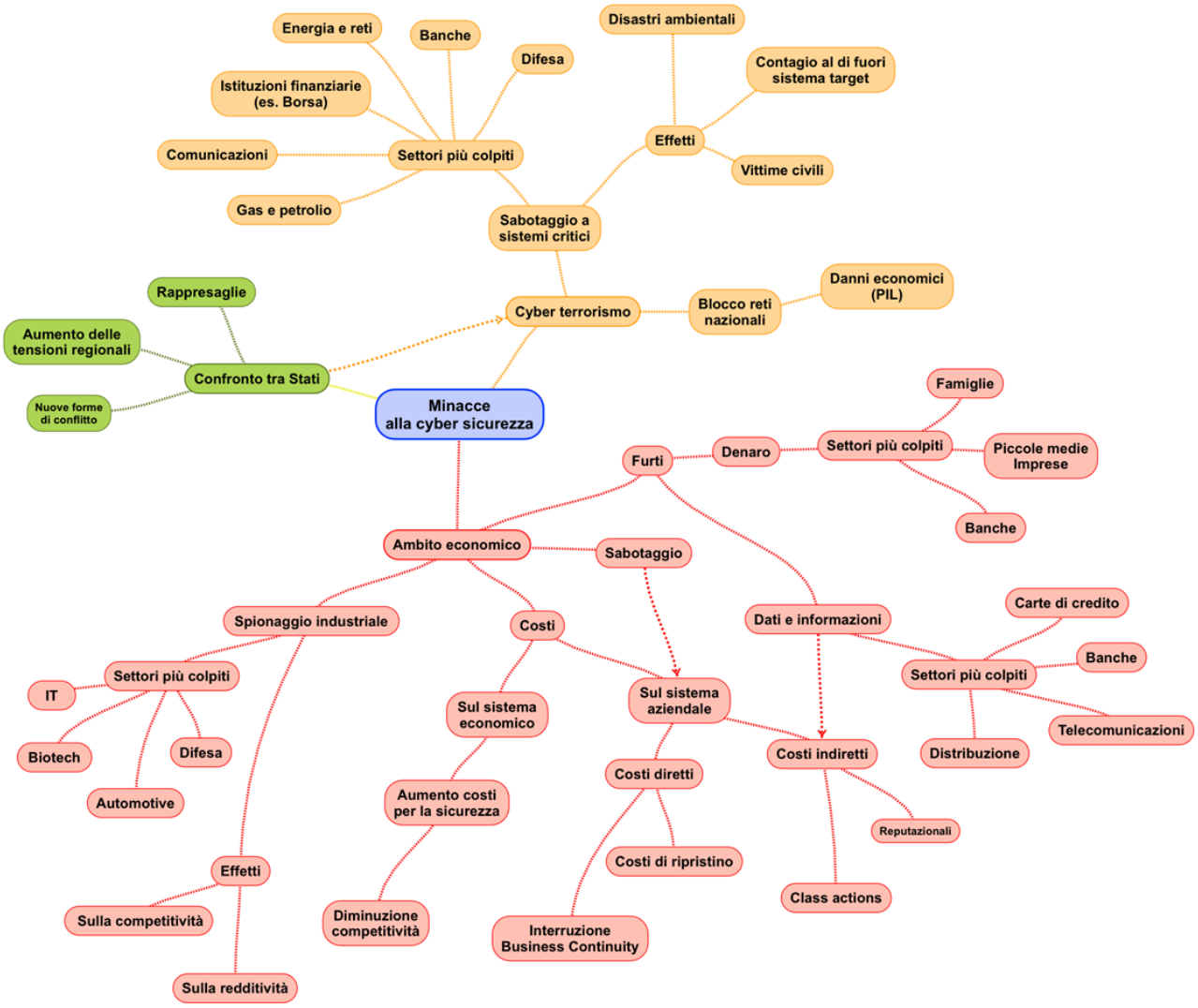
Il cyber spazio apre nuove potenzialità a chi ha interesse, per denaro o per obiettivi strategici e politici, ad attaccare gli Stati e le imprese più vulnerabili.

Volendo azzardare alcuni drammatici scenari evolutivi, il cyber spazio potrebbe tendenzialmente diventare terreno di un nuovo e più sofisticato terrorismo in grado di agire con gli stessi effetti distruttivi e psicologici del terrorismo reale. Oltre al blocco dei sistemi informatici di una nazione, che hanno fatto parlare di possibile *Cyber Pearl Harbour* si possono citare solo alcuni esempi che riguardano la manipolazione di sistemi informatici attivati per provocare devastanti effetti sul piano reale della vita delle persone.

Ad esempio gli analisti che si occupano di sicurezza hanno più volte presentato in letteratura alcuni scenari particolarmente catastrofici: quale sarebbe l'impatto di un attacco informatico in grado di manipolare i sistemi di controllo di una piattaforma petrolifera provocando una fuoriuscita di greggio, o ancora quali gli effetti di un sabotaggio ad una centrale nucleare?

Siamo davvero in un terreno nuovo anche del confronto tra gli Stati: fino a che punto potrebbe arrivare la reazione di un paese di fronte a una violazione dei propri interessi strategici?

Sicuramente quanto avviene nel cyber spazio apre a nuove categorie di rischi che dovremo abituarci ad assumere sia nelle analisi delle singole imprese, sia più in generale nella valutazione delle potenziali minacce sistemiche.


Energia e reti
Banche
Difesa
Disastri ambientali
Contagio al di fuori sistema target
Istituzioni finanziarie (es. Borsa)
Comunicazioni
Settori più colpiti
Effetti
Vittime civili
Gas e petrolio
Sabotaggio a sistemi critici
Rappresaglie
Cyber terrorismo
Blocco reti nazionali
Danni economici (PIL)
Aumento delle tensioni regionali
Confronto tra Stati
Nuove forme di conflitto
Minacce alla cyber sicurezza
Famiglie
Furti
Denaro
Settori più colpiti
Piccole medie Imprese
Banche
Ambito economico
Sabotaggio
Spionaggio industriale
Costi
Dati e informazioni
Carte di credito
Banche
Settori più colpiti
Telecomunicazioni
Distribuzione
IT
Settori più colpiti
Biotech
Difesa
Automotive
Sul sistema economico
Sul sistema aziendale
Costi indiretti
Costi diretti
Aumento costi per la sicurezza
Reputazionali
Costi di ripristino
Effetti
Class actions
Sulla competitività
Diminuzione competitività
Interruzione Business Continuity
Sulla redditività